IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A data recording and processing medium in at least one of a consumer electronic device and a personal computer, comprising:

copy protected digital data comprising:

- a passive part comprising content to be protected in encrypted form;
- an active part comprising information about how to decrypt the content comprised in the passive part; and
- a hidden part;

wherein the active part and the corresponding passive part constitute an active content and the hidden part is allocated to at least one of the active content, the active part of the active content and the passive part of the active content,

wherein the active part is adapted to automatically amend itself to build an amended active part each time at least one of decryption and encryption of the passive part is performed,

wherein the hidden part comprises information at least about properties of said active content, said active part and said passive part;

wherein the active part of the active content further comprises rules that either allow or forbid decryption of the content comprised in the passive part of the active content based on the information comprised in the hidden part,

wherein said data is residing on said data recording and processing medium, [[and]]

wherein said recording and processing medium pertains to at least one of [[a]] the consumer electronic device and [[a]] the personal computer[[.]], and

wherein the active part of the active content is adapted to permanently deny decryption of the content comprised in the passive part of the active content if the information comprised in the hidden part does not comply with the rules of the active part.

Claim 2 (Previously Presented): The data recording and processing medium of claim 1, wherein the active part is adapted to:

- read out the information comprised in said hidden part;
- compare said information with the rules; and
- perform or deny decryption of the content comprised in the passive part based on a comparison result.

Claim 3 (Canceled).

Claim 4 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active part further comprises information about how to encrypt decrypted content.

Claim 5 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active part is further adapted to perform at least one of decoding and reproduction of decrypted content after decryption of the content comprised in the passive part.

Claim 6 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active part is adapted to:

completely load and delete the passive part,

to decrypt and reproduce the content comprised in the loaded passive part,

to encrypt the decrypted content after reproduction, and

to store the encrypted content into a new passive part.

Claim 7 (Previously Presented): The data recording and processing medium of claim 6,

wherein

the active part is adapted to

perform loading, deletion, decryption, encryption and storing of the content comprised in the passive part in real time during reproduction of the content comprised in the passive part.

Claim 8 (Previously Presented): The data recording and processing medium of claim 6,

wherein

the active part is adapted to store the new passive part together with an adapted active part into a new active content.

Claim 9 (Canceled).

Claim 10 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active part is a tamper resistant software.

Claim 11 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the rules comprised in the active part comprise:

information about how often the content comprised in the passive part is allowed to be decrypted, and about how often the content comprised in the passive part has already been decrypted.

Claim 12 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the rules comprised in the active part comprise information about how long the content comprised in the passive part is allowed to be decrypted.

Claim 13 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the rules comprised in the active part comprise information about how often the content comprised in the passive part is allowed to be lend and how often the content comprised in the passive part has already been lend.

Claim 14 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active content comprises a data file operable by an operating system.

Claim 15 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the active part is adapted to separate the passive part from the active content for decryption of the content comprised in the passive part.

Claim 16 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the hidden part automatically is allocated to at least one of the active content, the active part of the active content and the passive part of the active content by an operating system.

Claim 17 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the hidden part is stored in a system file of an operating system.

Claim 18 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the hidden part is stored in encrypted form.

Claim 19 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the hidden part further comprises information about at least one of the location of the active content, the active part of the active content and passive part of the active content.

Claim 20 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the information comprised in the hidden part is automatically changed by an operating system to build an amended hidden part each time at least one of the active content, the active part of the active content, the passive part of the active content, the content comprised in the passive part of the active content is at least one of read out, amended, and stored.

Claim 21 (Previously Presented): The data recording and processing medium of claim 1,

wherein

the encrypted content comprised in the passive part is at least one of digitized audio data, digitized video data, digitized picture data, a database, a software, and digitized text.

Claim 22 (Canceled).

Claim 23 (Currently Amended): Method of reproducing a copy protected digital data in at least one of a consumer electronic device and a personal computer, the copy of protected digital data comprising:

- a passive part comprising content to be protected in encrypted form;

- an active part comprising information about how to decrypt the content comprised in the passive part; and

- a hidden part in the at least one of the consumer electronic device and the personal computer;

wherein the active part and the corresponding passive part constitute an active content,

wherein the hidden part is allocated either to the active content the active part of the active content and the passive part of the active content,

wherein the hidden part comprises information about at least one of the properties of said active content and/or respective active part and/or the respective passive part,

wherein the active part of the active content further comprises rules to allow and forbid decryption of the content comprised in the passive part of the active content based on the information comprised in the hidden part; and

wherein the active part of the active content is adapted to permanently deny decryption of the content comprised in the passive part of the active content if the information comprised in the hidden part does not comply with the rules of the active part;

the method comprising at least the following steps:

reading the information comprised in the hidden part of the copy protected digital data;

comparing said information with the rules comprised in the corresponding active part of the active content;

denying decryption of the content comprised in the passive part of the active content if the information read from the hidden part does not comply with the rules and terminating the method;

loading the encrypted content comprised in the passive part of the active content if the information read from the hidden part complies with the rules;

performing decryption of the encrypted content;

reproducing decrypted content; and

automatically amending the active part of the active content by control of the active part of the active content to build an amended active part each time decryption of the content comprised in the passive part is performed.

Claim 24 (Previously Presented): The method according to claim 23, wherein the method further comprises the steps of

deleting the passive part;

encrypting the decrypted content after reproduction; and

storing the encrypted content into a new passive part.

Claim 25 (Previously Presented): The method according to claim 24, wherein the step of reproducing the decrypted content, the step of deleting the passive part and the step of encrypting the decrypted content after reproduction are performed in real time during reproduction of the decrypted content.

Claim 26 (Previously Presented): The method according to claim 23, wherein the method further comprises the step of:

automatically amending the hidden part by control of an operating system to built an amended hidden part each time at least one of the active content, the active part of the active content the passive part of the active content the content comprised in the passive part of the active content is read, amended and stored.

Claim 27 (Canceled).

Claim 28 (Currently Amended): A ~~[software product residing and running on a data recording and processing means, comprising:~~

~~a series of state elements which are adapted to be processed by the data processing means such, that a method according to claim 23 may be executed thereon]~~ non-transitory computer readable storage device in at least one of a consumer electronic device and a personal computer having computer readable instructions thereon that when executed by a processor implement a series of state elements configured to implement:

- a passive part comprising content to be protected in encrypted form;
- an active part comprising information about how to decrypt the content comprised in the passive part; and

- a hidden part in the at least one of the consumer electronic device and the personal computer;

wherein the active part and the corresponding passive part constitute an active content,

wherein the hidden part is allocated either to the active content the active part of the active content and the passive part of the active content,

wherein the hidden part comprises information about at least one of the properties of said active content and/or respective active part and/or the respective passive part,

wherein the active part of the active content further comprises rules to allow and forbid decryption of the content comprised in the passive part of the active content based on the information comprised in the hidden part; and

wherein the active part of the active content is adapted to permanently deny decryption of the content comprised in the passive part of the active content if the information comprised in the hidden part does not comply with the rules of the active part;

and perform method steps including

reading the information comprised in the hidden part of the copy protected digital data;

comparing said information with the rules comprised in the corresponding active part of the active content;

denying decryption of the content comprised in the passive part of the active content if the information read from the hidden part does not comply with the rules and terminating the method;

loading the encrypted content comprised in the passive part of the active content if the information read from the hidden part complies with the rules;

performing decryption of the encrypted content;

reproducing decrypted content; and

automatically amending the active part of the active content by control of the active part of the active content to build an amended active part each time decryption of the content comprised in the passive part is performed.

Claim 29 (New): A non-transitory computer readable storage device according to claim 28, wherein said hidden part being invisible to a user and implemented as a component of an operating system executed by the at least one of the consumer electronic device and personal computer.